Published and Copyright (c) 1999 - 2011
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1318 05/06/11

~ LastPass Is Attacked? ~ People Are Talking! ~ Wii Gets Price Cut!
~ Sony Hacks Get Worse! ~ Mozilla: No Censor Help ~ Do Not Track Bills!
~ Sony's CEO Apologizes! ~ NZ-US Piracy Crackdown! ~ Fake MacDefender!

~ Pay Up Or Else Schemes ~ Generic Web Domains? ~ IE, Firefox Sliding!

-* Raid On bin Laden Is Tweeted! *-
-* Osama bin Laden's Death = Malware! *-
-* Building Better Passwords, Keeping Sanity! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"

Obviously, the biggest news of the week is the killing of Osama bin Laden! Regardless of your feelings about it, I believe that this action was just a matter of time. And, I believe that his death was planned as the only outcome of this raid.

Personally, I am relieved to know that this terrorist has met his end; and I'm not disappointed in how it occurred. That may sound callous, but this man did not deserve any form of mercy. The only feeling of disappointment that I have is that it took us almost ten years to get him.

I view bin Laden's death as simply a temporary "victory" against terrorism. Others will take his place, and terrorism will continue. As long as there are fanatics in the world who desire power and seek violent means to their perceived ends, terrorism will continue. Hopefully, the world will continue to recognize it as it occurs, and does what is necessary to defeat it.

On a much more calm topic, it looks like Spring weather may be here to stay for awhile. While we haven't had any drastic temperatures, the weather has been pretty good. Leaves are popping out on trees, flowers and plants are blooming, and even my lawn is starting to look good! Plenty of work to do to help repair damages from last summer's drought-like weather, but nature is doing its part to help the healing process.

I'll be going back to work at my second job, a seasonal one, at the local golf course. I'll be looking forward to working outside again, so we'll see how another season will go.

So, let's get going with another week here at A-ONE - enjoy the issue!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Sony: 25 Million More Hacked!
Sony CEO Apologizes for Massive Data Breach!

Nintendo Cuts Wii Price!
And more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""

Sony Says 25 Million More Accounts Hacked

Sony Corp. said Monday that hackers may have taken personal information from an additional 24.6 million user accounts after a review of the recent PlayStation Network breach found an intrusion at a division that makes multiplayer online games.

The data breach comes on top of the 77 million PlayStation accounts it has already said were jeopardized by a malicious intrusion.

The latest incident occurred April 16 and 17 - earlier than the PlayStation break-in, which occurred from April 17 to 19, Sony said.

About 23,400 financial records from an outdated 2007 database involving people outside the U.S. may have been stolen in the newly discovered breach, including 10,700 direct debit records of customers in Austria, Germany, the Netherlands and Spain, it said.

The outdated information contained credit card numbers, debit card numbers and expiration dates, but not the 3-digit security code on the back of credit cards. The direct debit records included bank account numbers, customer names, account names and customer addresses.

Company spokeswoman Taina Rodriguez said Sony had no evidence the information taken from Sony Online Entertainment, or SOE, was used illicitly for financial gain.

"We had previously believed that SOE customer data had not been obtained in the cyber-attacks on the company, but on May 1 we concluded that SOE account information may have been stolen and we are notifying you as soon as possible," Sony said in a message to customers.

Sony said that it shut service Monday morning to Sony Online Entertainment games, which are available on personal computers, Facebook and the PlayStation 3 console. Its most popular games include "EverQuest," "Free Realms" and "DC Universe Online."

The company said it will grant players 30 days of additional time on their subscriptions, along with one day for each day the system is down. It is also creating a "make good" plan for its multiplayer online games.

On Sunday, Sony executives bowed in apology and said they would beef up security measures after an earlier breach caused it to shut down its PlayStation network on April 20. The company is working with the FBI and other authorities to investigate what it called "a criminal cyber attack" on Sony's data center in San Diego, Calif.

The company said it would offer "welcome back" freebies such as

complimentary downloads and 30 days of free service to PlayStation customers around the world to show remorse and appreciation.

PlayStation spokesman Patrick Seybold, in a blog post Monday, denied a report that said a group tried to sell millions of credit card numbers back to Sony.

He also said that while user passwords had not been encrypted, they were transformed using a simpler function called a hash that did not leave them exposed as clear text.

Sony CEO Apologizes for Massive Data Breach

Sony Corp. Chief Executive Howard Stringer apologized for "inconvenience and concern" caused by the security breach that compromised personal data from more than 100 million online gaming accounts.

In a blog post late Thursday, the head of the Japanese technology giant sought to reassure customers, saying the company is focused on investigating and fixing the hacker attack.

"We are absolutely dedicated to restoring full and safe service as soon as possible and rewarding you for your patience," Stringer wrote in his first public comments since Sony shut down its PlayStation Network on April 20.

Stringer said there is "no confirmed evidence" that stolen information has been misused.

He acknowledged criticism that Sony was slow to inform customers of the embarrassing breach, calling the issue a "fair question." As soon as the company discovered the potential scope of the problem, it suspended the network and hired technical experts to help, he said.

The network serves both the PlayStation video game machines and Sony’s Qriocity movie and music services. The system links gamers worldwide in live play, and also allows users to upgrade and download games and other content.

Although Sony began investigating unusual activity on the PlayStation network on April 19, it did not notify consumers of the breach until April 26.

"I wish we could have gotten the answers we needed sooner, but forensic analysis is a complex, time-consuming process," Stringer said. "Hackers, after all, do their best to cover their tracks, and it took some time for our experts to find those tracks and begin to identify what personal information had - or had not - been taken."

Sony has said the attack may have compromised credit card data, email addresses and other personal information from 77 million user accounts. On Monday, it said data from an additional 24.6 million online gaming accounts also may have been stolen.

Along with assurances that it is strengthening security measures, Sony is enticing potentially wary customers with a "welcome back" program that includes complimentary entertainment downloads and a 30-day

membership to its PlayStation Plus premium service.

It also launched an identity theft protection program for U.S. account holders. The service includes a $1 million identify theft insurance policy and will be free for 12 months after enrollment.

Sony signaled in a separate blog post Thursday that service could be restored soon. The company said it is in the "final stages of internal testing of the new system," though did not offer a specific timeline.

Nintendo Cuts Wii Price, Offers Cheaper Game Set

Nintendo is dropping the price of its Wii game system by $50 to $150 and introducing a new line of cheaper Wii games.

Starting May 15, the newly priced Wii system will come in either black or white with a "Mario Kart Wii" game and a Wii Wheel accessory, replacing the previously included "Wii Sports" and "Wii Sports Resort" games.

The price cut - the second one since the Wii launched for $250 in 2006 - comes less than a month after the Japanese company announced the console will have a successor next year. Nintendo Co. said in late April it will show off a playable model of the new system at the Electronic Entertainment Expo, which runs June 7-9 in Los Angeles.

The company said Wednesday that the "Nintendo Selects" collection of games will come with a suggested retail price of $20. The four games include "The Legend of Zelda: Twilight Princess," "Animal Crossing: City Folk," "Mario Super Sluggers and Wii Sports." It’s the first time "Wii Sports" will be sold separately rather than packaged with the Wii.

The Wii redefined gaming when it launched nearly five years ago, expanding video game audience by offering intuitive motion controllers instead of complex buttons. But the Wii isn’t as technologically powerful as its counterparts from Sony and Microsoft, the PlayStation 3 and the Xbox 360. Unlike those two, it doesn’t offer high-definition images.

Nintendo has not given details on the capabilities of the new console.

New Installment of "Assassin’s Creed" On Its Way

Ubisoft on Thursday revealed that the latest installment of its beloved series of "Assassin’s Creed" videogames will be released in November.

The French videogame powerhouse promised a glimpse at "Assassin’s Creed Revelations" at a premier Electronic Entertainment Expo in early June in Los Angeles.

"Revelations" will be the fourth videogame in a series that has sold more than 28 million copies overall since the first title was released in 2007.

Players will continue on as fictional master assassin Ezio Auditore, this time in the heart of the Ottoman Empire to foil enemies in Constantinople.

"Delivering the final chapter of the Ezio trilogy is an important milestone in the Assassin's Creed franchise for us and for our fans," said Ubisoft Montreal creative director Alexandre Amancio.

He promised that the game will deliver "lots of new features and some significant surprises."

"Revelations" will be released in November with versions tailored for play on Xbox 360 or PlayStation 3 consoles as well as personal computers running on Windows software.

"Assassin's Creed" was the first game to immerse players in a believable and mature experience inspired by historical events, according to Ubisoft videogame producer Sebastien Puel.

The second installment of the videogame introduced Auditore and combined the original title's winning elements with more gorgeous cityscapes, animations, and 15th century historical settings.

"Assassin's Creed: Brotherhood" released last year built on the Renaissance era treachery and intrigue of its predecessor, but with a first-ever online feature that allows players to divert from the storyline and hunt one another.

The multi-player feature was incorporated into "Revelations."

Players can opt for a storyline mode that puts them in the trademark hooded garb of Ezio, part of a bloodline of master assassins that used their deadly skills to thwart corruption and grand conspiracy.

The "Assassin's Creed" franchise has grown to include novels, comic books, and short films.

More information is available online at assassinscreed.com or facebook.com/assassinscreed.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Captured on Twitter: Raid Against Osama bin Laden

In the early hours of Monday, Sohaib Athar reported on Twitter that a loud bang had rattled his windows in the Pakistani town of Abbottabad, adding that he hoped it wasn't "the start of something nasty.

A few hours later Athar posted another tweet: "Uh oh, now I'm the guy

who liveblogged the Osama raid without knowing it."

In the age of Twitter, perhaps it’s no surprise that the first signs of the U.S. operation that killed al Qaeda leader Osama bin Laden were noticed by an IT consultant awake late at night.

Athar, a resident of Abbottabad where bin Laden was holed up in a fortified mansion, first noticed the sound of a helicopter and thought it unusual enough to post via his Twitter account.

"I was awake, working on my computer when I heard a sound of helicopter. It was rare here. It hovered for about six minutes and then there was a big blast and power gone," Athar, 34, said in an interview with Reuters.

"I tweeted it because it was something unusual in the city," said Athar, adding that he moved from Lahore to the city a year and a half ago to avoid "bomb blasts and terrorist attacks."

After liveblogging and speculating for several hours over what happened, it dawned on Athar and those following him that they were witnessing the end of a worldwide manhunt for the man held responsible for orchestrating the September 11, 2001 attacks.

"I think the helicopter crash in Abbottabad, Pakistan and the President Obama breaking news address are connected," said one of Athar’s followers.

Seven hours after Athar’s first tweet, President Barack Obama announced bin Laden’s death in an operation by U.S. forces where one helicopter was lost.

Twitter, launched five years after the 2001 attacks, is used by an estimated 200 million people per day, serving as an internet platform for users to broadcast, track and share short messages of no more 140 characters in length.

Athar’s tweets, initially peppered with jokes ("Uh oh, there goes the neighborhood") eventually turned to exasperation as his email inbox, Skype and Twitter accounts were flooded by those trying to reach him ("Ok, I give up. I can’t read all the @ mentions so I’ll stop trying").

The number of people following Athar, whose Twitter handle is "ReallyVirtual," ballooned to nearly 33,000 later on Monday, from several hundred before.

Athar also runs a coffee shop in the center of Abbottabad, across from the Army Burn Hall College school in the same neighborhood as bin Laden’s mansion. He fears that his new hometown, a relatively affluent enclave about 35 miles north of Islamabad, could now come under attack.

"They can attack military installation and this city has more targets than anywhere else," Athar said.

Separately, in the United States, the first indication that bin Laden had been found and killed came from a another tweet by Keith Urbahn, who says on his Twitter profile that he is chief of staff for former Defense Secretary Donald Rumsfeld.

"So I’m told by a reputable person they have killed Osama Bin Laden. Hot damn," Urbahn tweeted more than an hour before Obama’s speech.

Online Scammers Jump on bin Laden News

Online thieves and spammers are using the killing of Osama bin Laden to send out malicious software and spam to unwitting Internet users.

In what's become common practice among the Internet's less savory citizens, these scammers are sending out emails and spreading Facebook posts that purport to be videos or photos of the dead bin Laden.

They are not. But by clicking the links, users can download computer viruses that steal personal information or otherwise infect their computers.

Computer security firm Symantec says one spam email contains a link to bogus photos and videos purporting to be from CNN Mexico. Instead, it directs people to a scam site designed to look like the real thing but created to steal passwords. Some Facebook users also fell victim to fake bin Laden links that then spread the links to their friends' pages on the site.

The FBI warned Internet users of the scams Tuesday. On Wednesday, President Barack Obama said he has decided not to release photos of the dead bin Laden because they could incite violence and create national security risks for the U.S.

That didn't stop Internet scammers from spreading fake, doctored photos to lure people into giving away their personal information or downloading the troublesome programs known as "malware."

Symantec senior manager David Cowings said spammers are "pretty opportunistic," using everything from scare tactics to celebrity gossip to pandering to mere raw curiosity to send out their messages. Some of these Internet ruses pre-date the nearly decade-long hunt that culminated in bin Laden's death.

"They'll frequently spoof well-known news organizations to make (the) email more legitimate," just as they did in the case of CNN.

Avoiding scams is best done by practicing "good Internet hygiene," Cowings said. That means avoiding questionable sites by reading their URL, or address, from left to right. Sometimes the first few letters of a site will look legitimate but subsequent ones will raise red flags. Also be suspicious of sites prompting you to install video-viewing software or antivirus protection. Sometimes bad links will be packaged with a prompt to download something, saying your software is not up to date, Cowings said. It's safer to go directly to the website that offers the software.

Common sense is another good tool. Is your staid college professor writing "LOL, check it out!!!" on a Facebook link? If it's not characteristic for a person to write that way, chances are they didn't type it. Having up-to-date security software is also crucial. This can protect your computer from viruses even if clicking on a bad link that attempts to download malware.

US Lawmakers Plan ’Do Not Track’ Bills

US lawmakers announced plans on Friday to introduce "Do Not Track" legislation that would let Internet users block companies from gathering information about their online activities.

Senator Jay Rockefeller, a Democrat from West Virginia, said his "Do Not Track Online Act of 2011" will offer a "simple, straightforward way for people to stop companies from tracking their every move on the Internet."

"Consumers have a right to know when and how their personal and sensitive information is being used online - and most importantly to be able to say ’no thanks’ when companies seek to gather that information without their approval," Rockefeller said in a statement.

In the House of Representatives, Joe Barton, a Republican from Texas, and Edward Markey, a Democrat from Massachusetts, released a draft of a separate "Do Not Track" bill aimed at protecting children online.

US senators John Kerry and John McCain introduced an online privacy bill last month that would require companies gathering data to allow a consumer to "opt-out" of having their information collected.

The former Democratic and Republican presidential candidates said their bipartisan bill seeks to strike a balance between protecting the personal information of Web users and the needs of businesses to conduct electronic commerce.

The flurry of legislation comes amid a series of high-profile data theft incidents, including the theft of personal information from more than 100 million Sony accounts, and controversy over tracking technology in Apple’s iPhone and in smartphones running Google’s Android software.

Apple and Google have been invited to attend a congressional hearing on privacy next week following claims the iPhone and Android devices regularly track a user’s location and stores the data.

Rockefeller, chairman of the Senate Commerce Committee, said his bill would create a "legal obligation" for all online companies to honor the choice of consumers who say they do not want to be tracked online.

It would give the Federal Trade Commission the power to pursue any company that does not honor the request.

Barton and Markey, the co-chairmen of the Bi-Partisan Congressional Privacy Caucus, said their "Do Not Track Kids Act of 2011" establishes new protections for the personal information of children and teenagers.

"For millions of kids today, the Internet is their new 21st century playground," Markey said in a statement. "But kids growing up in this online environment also need protection from the dangers that can lurk in cyberspace."

Barton said the Internet has "transformed into an invaluable educational, research and entertainment tool, but with the good comes the bad.

"I strongly believe that information should not be collected on children and used for commercial purposes," he said.

The bill would notably require online companies to obtain parental consent before collecting children’s personal information and prohibit them from using personal information of children and teens for targeted marketing.

It would also create an "Eraser Button" for parents and children that would allow users to eliminate publicly available personal information content "when technologically feasible."

Jeff Chester of the Center for Digital Democracy welcomed the bill, saying "young people are targets of a powerful digital data collection system, tracking them wherever they are - on mobile phones, social networks, playing games, or browsing the Web.

"We need a 21st century privacy law that protects children and teens," Chester said.

How to Build Better Passwords Without Losing Your Mind

Your e-mail password is your last line of defense when it comes to online privacy and security; if a hacker cracks that, they could potentially reset the passwords of and gain access to your social networks, your bank account and even your identity by taking advantage of the ubiquitous "I Forgot My Password" button.

It’s tempting to use the same password for all of your online accounts, but doing so renders every account vulnerable if any one of them gets hacked. But given some recent massive security breaches, now’s a good time to update your passwords and make sure each is unique.

There are a few great password management programs like KeePass that will store all of your passwords in one encrypted database and allow you to access them with one master password, allowing you to carry every password you ll ever need on a single thumb drive. A multi-platform password manager with browser support like LastPass is even easier to use because it will automatically sync between different computers and browsers, letting you access your encrypted database from any device, though you sacrifice the security of keeping your password list confined to a single hard drive.

Using a password manager is a great way to improve your personal security online, but it s not perfect; the perfect password is the one you never write down, a unique string of letters, numbers and symbols that not even you know until the moment you enter it. That may be beyond our grasp, but you can get awful close by using a few simple mnemonic tricks.

It s actually fairly easy to create strong, unique passwords by following a few simple rules. First, we need a password "base" with a mix of upper and lower case letters, numbers and even a symbol or two to spice things up. Pick a phrase that will be easy to remember, and feel free to be as creative as you like. For simplicity s sake I m going to use one of my favorite dishes, chicken adobo, as our example.

Make sure your passphrase is at least eight characters and avoid obviously memorable topics like proper names, birthdays and hometowns. You should also avoid picking a single word and changing some of its characters to symbols - hacker tools are sophisticated enough to foil that trick. Go for

a passphrase - multiple words strung together - rather than a password; this makes it harder for hackers working to crack your password by trying every word in the dictionary.

Now that we ve picked a passphrase, we need to mash that phrase into a single string (chickenadobo), then sprinkle in a few capital letters that are simple to remember (ChickenAdobo). Next, let s pepper our password base with a few random characters to keep things interesting (Ch!cken@dob0).

Now that we have our base password, we re going to memorize and use it as a skeleton key that will unlock our account on any Website as long as we hold fast to a few simple rules. To create the strongest password possible, we re going to invent a simple naming pattern as a mnemonic device that will help us generate a unique password for every Website we visit.

For example, let s say I decided to always use the first and fourth letter of a Website s domain name in the middle of my passphrase, capitalizing the former while leaving the latter lower-case. That means my Facebook.com account would have the unique password Ch!ckenFe@dob0, while my about.me account would require the password Ch!ckenAu@dob0.

See the pattern? Make up a something similar and you ll have a unique alphanumeric password for every website you visit, one that s easy to remember but nearly impossible for hackers to figure out. No password is perfect, but knowing your own unique passphrase and a few mnemonic tricks will go a long way towards keeping your online privacy intact.

Assuming ’The Worst,’ LastPass Urges Password Change

It’s the Age of Security Breaches. Password-management service LastPass said Thursday it may have been attacked, and the company issued a warning to users to change their master passwords.

On its company blog, LastPass said it noticed on Tuesday morning a "network traffic anomaly for a few minutes from one of our noncritical machines." It said such anomalies "happen occasionally, and we typically identify them as an employee or an automated script." LastPass provides cross-platform storage of passwords.

But, the company said, it couldn’t locate the root cause for this anomaly. It then found a "similar but smaller matching traffic anomaly from one of our databases in the opposite direction," meaning traffic received by the server.

Since it couldn’t account for the issue, LastPass said it was "going to be paranoid and assume the worst" - namely, that the database had been accessed.

The company said users who have a "strong, non-dictionary-based password or passphrase" shouldn’t be impacted. If there is a threat, the company said, it’s that someone will try to crack passwords using dictionary words.

But, to be safe, the company at first required all users to change their master passwords, and to do so either by using a previously used IP address - meaning logging on from the same network connection as was

previously used - or validating an e-mail address.

The directive to its millions of users, however, overloaded the company's servers. To avoid overload, the company has allowed people to let the company know if their master password is non-dictionary-based and therefore not in need of changing, in addition to other ways of communicating with the company.

LastPass CEO Joe Siegrist has told news media that he may have been "too alarmist" in his response. He indicated that the anomaly was the transfer of a substantial amount of data between machines that wouldn't normally show such traffic.

But the continuing saga of Sony's networks has made companies very aware of the need to speedily respond to possible intrusions. Starting on April 20, Sony's PlayStation Network, Qriocity music service, and Sony Online Entertainment networks have been down because of what Sony has described as an "external intrusion."

Days after the initial outage, Sony revealed that confidential data from millions of users may have been taken - possibly as many as 100 million users, which would make it the largest ID theft in history.

The size of the potential ID heist, and Sony's slow response in directly informing users, has elicited a storm of investigations and criticism. A congressional subcommittee, the New York attorney general, at least one U.S. senator, and a privacy official in Germany have either begun investigations or asked for more information, and at least two class-action suits have been filed.

Mozilla Refuses to Help Censor the Internet

Mozilla, maker of the open source Firefox browser, recently told the Department of Homeland Security that if you want to censor the Internet you better have a good reason or at least a legal justification. U.S. Immigration and Customs Enforcement, the DHS' principal investigative arm, recently asked Mozilla to remove an add-on called MafiaaFire Redirector from the organization's Firefox add-ons site.

The government agency said MafiaaFire was circumventing a series of ICE domain seizures.

MafiaaFire exes seized domains and then redirect users to active sites that use the same name but now operate under a different Web address. If you went to Torrent-finder.com, for example, you'd see a site seizure notice, but the actual site is still alive under the same name as an ".info" site. The same can be said for many of the sites ICE has seized. So MafiaaFire acts as an automated navigation system to help users find their way down the Web's dark alleys.

Mozilla's legal department didn't immediately comply with ICE's request to take down MafiaaFire and instead asked for more clarification. "Our approach is to comply with valid court orders...but in this case there was no such court order," Harvey Anderson, a member of Mozilla's legal team, recently explained on his personal blog. "Thus, to evaluate Homeland Security's request, we asked them several questions...to understand the legal justification."

Mozilla posed a series of eleven questions to DHS about their request to take down MafiaaFire such as have any courts determined that MafiaaFire is illegal? Is Mozilla legally obligated to take down MafiaaFire? And, has the government talked to MafiaaFire about its concerns?

So far, DHS has not responded to Mozilla's request for more information. Mozilla posed its questions to DHS on April 19.

ICE has been hard at work in recent months shutting down sites such as TV Shack, Torrent-finder.com, Ninja Video, and many others for violating U.S. copyright law. These sites typically index pirated video streams hosted on services such as Megavideo and VuReel or function as search engines for file-sharing torrents.

The problem is once ICE shuts a copy-infringing site down, it will often pop back up within hours under the same name but with a new top-level domain (.com, .info, .org, etc.). MafiaaFire's purpose, at least in part, is to demonstrate the futility of shutting down these sites.

Digital rights groups such as the Electronic Frontier Foundation and the Center for Democracy and Technology have criticized ICE's practice of seizing domains.

Fake "MacDefender" Brings Malware to Macs

Fake anti-virus software is an old breed of malware that's finally found a new trick: Attacking Macs.

The malicious Mac app is called MacDefender, and according to Intego, it hides within Web pages that use search engine optimization to spam the results of popular searches. Infected Websites show a fake animation of a malware scan in Windows, followed by a pop-up telling users that their computer is infected. JavaScript on the page then automatically downloads a compressed ZIP file containing the malware.

For Safari users who've checked the "open 'safe' files after downloading" option within the browser's settings, the MacDefender malware installation begins automatically. Otherwise, the user must open the ZIP file and install the app manually for the malware to take hold.

the software developer of the same name - looks rather convincing, and once installed, it quickly sets to work on discovering non-existent viruses and loading pornography in the user's Web browser. The point of all this is to scare users into forking over their money and credit card information, which the MacDefender app says is necessary to delete viruses.

Fortunately, Intego describes this Mac malware as low risk and not very widespread for now. It's also fairly easy to remove, as The Next Web points out to disable anything related to MacDefender. Then, make sure there are no references to the malware app in Library/StartupItems or, in the same place, LaunchAgents and LaunchDaemons. Then, move the MacDefender app from Applications to Trash, and delete the trash. Finally, use Spotlight Search to find and delete any remaining references to the app.

For prevention, Intego recommends its own anti-virus software (of course), but all you really need is common sense. Uncheck the "open

’safe’ files after downloading" option in Safari and never, ever install anti-virus software that pops up on some random website, no matter how many viruses it says your computer has.

WikiLeaks: US Offered To Bankroll New Zealand Piracy Crackdown

Making your country’s views known is a principal function of foreign embassies, but the US goes much further. According to cables released by WikiLeaks, the US embassy in New Zealand urged Uncle Sam to fork over about half a million New Zealand dollars back in 2005 to bankroll a private intellectual property enforcement unit run by major rightsholders in the region.

Operated on an informal basis by the Recording Industry Association of New Zealand (RIANZ) and the Australasian Mechanical Copyright Owners Society (AMCOS), the US identified the "unit" as the only potential bulwark against music piracy in the region.

"It is developing an intelligence framework to identify local producers of pirated works, distributors, criminal networks and recipients and to work with relevant government, law enforcement, customs and other authorities and stakeholders," the embassy’s cable noted. "The unit aims to prevent piracy by sharing intelligence with other organizations and agencies, lobbying political parties and the judiciary on the harm to industry and supporting public awareness campaigns."

The outfit would also launch "enforcement operations" targeting makers and distributors of illegal material, and it would "train law enforcement and other agencies in the implementation of intellectual property legislation through identifying offenses and disrupting piracy activities."

The cable drew up a recommended budget of NZ$533,000 (US $386,158) for the operation, with over $200,000 going to salaries and the rest funding start-up and operating costs. A proposed US budget for the New Zealand/South Pacific IP enforcement program.

Did any of this money get spent? If it had, it would have come from the US’s Intellectual Property Rights Training Program, mentioned as the proper source in the cable. We did an IPR database search for RIANZ and AMCOS, but couldn’t find either group listed, although a slew of other training programs popped up.

But this isn’t the only way that the US tried to wield influence on the region; it’s also willing to help countries write their laws. A May 2009 cable indicates that the US pretty much offered carte blanche help to New Zealand as it was rethinking its "three strikes" illegal file sharing law. "Embassy in the meantime has repeated its offer of assistance to [Government of New Zealand] officials to offer consultations with [United States Government] copyright experts through a [Digital Video Conference]," the missive explained.

As we reported at the time, New Zealand’s government eventually yanked the punitive Section 92A of the bill, denounced by content providers and ISPs as vague and impossible to implement. But the US seemed confident at the time that New Zealand would eventually come through with a new edition of the law.

Embassy officials also made clear their irritation with those who opposed industry-friendly copyright changes.

In the meantime, the IPR community has engaged the services of Price Waterhouse consultants to do a cost-benefit analysis on the potential losses to the NZ economy if the new S92A fails to be enacted. The IPR industry wants to be prepared to counter any false claims by opponents of the new provision who successfully managed to monopolize the local media's attention in the last round.

In the end, the US Trade Representative decided not to put New Zealand on its Special 301 Priority list - the watchdog list for countries of whose IP standards the US does not approve.

"While there is additional work to be done to strengthen the law and enhance enforcement," a March 2009 cable concluded, "Post recommends the better course of action is to continue engagement with the GNZ and monitor the progress of IP legislation rather than place New Zealand on this year's watch list."

IP-Address Is Not a Person, BitTorrent Case Judge Says

A possible landmark ruling in one of the mass-BitTorrent lawsuits in the U.S. may spell the end of the "pay-up-or-else-schemes" that have targeted over 100,000 Internet users in the last year. District Court Judge Harold Baker has denied a copyright holder the right to subpoena the ISPs of alleged copyright infringers, because an IP-address does not equal a person.

In the last year various copyright holders have sued well over 100,000 alleged file-sharers in the United States alone. The purpose of these lawsuits is to obtain the personal details of the alleged infringers, and use this information to negotiate a settlement offer ranging from a few hundred to a few thousand dollars.

Lawyers, the public and consumer advocacy groups have compared these practices to extortion, but nonetheless new cases are still being filed every month. This week, however, an interesting ruling was handed down by District Court Judge Harold Baker that, if adopted by other judges, may become a major roadblock for similar mass-lawsuits.

In the case VPR Internationale v. Does 1-1017, the judge denied the Canadian adult film company access to subpoena ISPs for the personal information connected to the IP-addresses of their subscribers. The reason? IP-addresses do not equal persons, and especially in adult entertainment cases this could obstruct a fair legal process.

Among other things Judge Baker cited a recent child porn case where the U.S. authorities raided the wrong people, because the real offenders were piggybacking on their Wi-Fi connections. Using this example, the judge claims that several of the defendants in VPR s case may have nothing to do with the alleged offense either.

"The infringer might be the subscriber, someone in the subscriber s household, a visitor with her laptop, a neighbor, or someone parked on the street at any given moment," Judge Baker writes.

Although the above logic applies to all BitTorrent lawsuits that are currently ongoing, the matter becomes especially delicate when the alleged offense is sharing rather explicit adult titles.

"Orin Kerr, a professor at George Washington University Law School, noted that whether you re guilty or not, you look like a suspect. Could expedited discovery be used to wrest quick settlements, even from people who have done nothing wrong?" Judge Baker writes.

Judge Baker further notes that "the embarrassment of public exposure might be too great, the legal system too daunting and expensive, for some to ask whether the plaintiff VPR has competent evidence to prove its case."

Baker concludes by saying that his Court is not supporting a "fishing expedition" for subscribers details if there is no evidence that it has jurisdiction over the defendants.

Although the ruling is definitely a setback for the copyright holders in mass-BitTorrent lawsuits, it has yet to be seen whether other judges will reach the same conclusion in future cases. If that happens, the end of this type of lawsuit in the U.S. may be near.

Texas lawyer Robert Cashman, who represents several defendants in similar lawsuits, agrees that the ruling can be a potential game changer.

"We may have just seen the order that may end all future John Doe lawsuits," he commented in a response.

Internet Explorer and Firefox Continue to Slide

New browser shows that both Internet Explorer and Firefox lost ground in April. While Microsoft and Mozilla trumpet their latest browsers, publicly trade jabs, and beat their chests at one another, Chrome and Safari are quietly gaining market share.

Firefox declined by nearly two tenths of a percentage point overall, while Internet Explorer fell just over eight tenths of a percentage point to a new low of 55.11 percent. IE still has two and a half times the market share of its closest competitor - Firefox - but it has been losing ground slowly, but surely over the past year or two.

Meanwhile, Chrome - which is the third place browser with a little less than 12 percent of the overall market - has seen a 65 percent increase in its piece of the pie since last June - climbing nearly five percentage points. Apple’s Safari browser isn’t doing too bad either with a nearly 50 percent increase over its June 2010 market share - most likely a reflection of the success of Apple’s iPhone and iPad.

For Firefox, there is good news for the latest version, but still disappointing news for the browser overall. Firefox 4 market share more than tripled from 1.68 percent to 5.43 percent. However, those gains were almost entirely wiped out by the drop in Firefox 3.6 - an indication that most of the Firefox 4 growth is coming from cannibalizing existing Firefox market share. Add in some minor losses by other Firefox versions and you have a slight drop in overall market despite the impressive gains of Firefox 4.

It is a similar story at Microsoft. IE9 more than doubled its global market share over March - coming in at 2.41 percent. However, the decline in IE8 market share is virtually equal to the IE9 gain - again seeming to show direct cannibalization of IE8 users. At the same time, IE 6 and IE 7 usage declined as well, but the decision by Microsoft to limit IE9 to only Windows 7 and Windows Vista means that many of those IE6 users are jumping to alternative browsers.

Because IE9 has a limited audience, Microsoft likes to view the data through that lens. If you narrow the scope of the discussion to only Windows 7, IE9 has a more impressive 7.46 percent - more than double the share it had on Windows 7 the previous month. It is interesting, however, to note that Firefox 4 actually has a larger presence on Windows 7 than Microsoft's IE9.

Still, if IE9 can just replace IE8 for Windows users, as the general population continues to migrate from Windows XP and embrace Windows 7 it will work in Microsoft's favor eventually.

Are You Ready for .anything? Generic Internet Domains on the Way

If you're an individual, a business, a Fortune 500 company - what do generic top-level domains mean for you? A headache, that's what.

In the 1990s, the race to stake a claim on the Web lay mainly in one direction: .com. Now, more than a decade later, that race may be more like an Easter egg hunt - a frantic sprint to collect as many top-level domains (TLDs) as possible. But those eggs cost money to hold onto - a lot of it. Oh, and the rules aren't quite written yet, either.

At a House subcommittee hearing on Wednesday morning, representatives of various industry groups will attempt to convince lawmakers that the Internet Center for Assigned Names and Numbers (ICANN) is ramming through what might be called "dot-anything" - generic domains from .airplane to .zebra, and everything in between.

Here's what businesses and individuals need to know, experts say: if you want to own your TLD, you'd better register it - and it will cost about the price of a house. Large companies like McDonalds should register ".mcdonalds", as then the giant hamburger chain can control every proposed domain name that includes the .mcdonalds suffix, experts say. Smaller businesses can survive, too, by banding together. And individuals? Unless your discretionary income is above six figures, forget it - a .com domain will suit you just fine.

The question, however, is how far should the process go? Does McDonalds need to own ".bigmac," ".mcd," or ".burger"? How about ".fastfood"? And that's where it gets tricky.

At that point, some fear, the land rush that gobbled up .com addresses will shift to generic TLDs. A version of that is going on now, with the March approval of the .xxx domain, which the adult industry vehemently fought and lost.

What's clear, however, is that the day of the gTLD is arriving soon. At the the House Committee on the Judiciary's Subcommittee on Intellectual Property, Competition, and the Internet hearing on Wednesday,

representatives from ICANN will square off against representatives from industry groups. Thousands of miles to the west, Digital Hollywood Spring will hold a session the same day to discuss the potential impact of a .music domain on Hollywood. And in mid-May, the International Trademark Association will address the gTLD issue in its own annual meeting.

Finalizing the process of applying for generic TLDs has taken years. In March, ICANN said that the guidebook for applying for a TLD would be finalized in June.

ICANN's position is that it's time to move gTLDs forward. When ICANN put forward the June timeframe, one of the members of the executive committee, Rita Rodin Johnston, an intellectual property lawyer and partner with Skadden Arps, said: "I think there has been a lot of talk and a lot of very robust debate on all sides of the issues. But I think if we continue, we can talk forever."

Industry executives expect that once the process opens, ICANN will process gTLD applications as fast as it can, to the tune of about 400 to 500 in the first round, and possibly up to 1,000 per year.

For $185,000, the fee ICANN set in 2008, you too can apply for a generic TLD - probably out of the reach of all but the wealthiest individuals, but one small businesses may have to consider. And that's if the TLD is available; applicants may have to bid for the proposed domain, and incur the costs of administering it.

The process is the same for a top-level domain used by billions of people; a so-called ".brand" TLD intended to serve a single registrant; or an open, unrestricted Latin character TLD in the mode of .com, Steven Metalitz, the counsel for the Coalition for Online Accountability, will testify in front of the House subcommittee. COA participants include the MPAA, RIAA, and the Software and Information Industry Association (SIIA) - perhaps the three most powerful intellectual-property groups in the world.

For enterprises, owning your own gTLD is a no-brainer, according to Ben Crawford, chief executive of CentralNIC and dotBrand Solutions, which will acquire and manage the TLD for clients.

"The typical trademark owner would love to have their own top level domain," because they become the gatekeeper for all domains with that suffix, Crawford said. "Every domain is under your complete control, with no fraud or phishing. It ends with the dot-brand. There's no consumer confusion."

That's not the case with generic .com, .net, or overseas addresses like .co.uk. While McDonalds could prohibit yucky.mcdonalds, it might have to litigate to force yuckymcdonalds.com out of business, or just buy up the domain itself. Misspellings, derivatives, and "typosquatting" remain problems in the established TLDs, and in the new .XXX domain as well.

"Disney.xxx is not a good thing for Disney," noted Nao Matsukata, senior policy adviser to the Coalition Against Domain Name Abuse (CADNA) and to Alston & Bird, LLP.

According to COA's Metalitz, the new generic TLD contain some small level of safeguards against abusive domain-name registrations: a "sunrise" period where trademark or brand holders can pre-emptively file for domain names identical to their trademarks, as well as an IP claims

service where second-level domain-name holders are warned if they share the same name as another party. Confusingly similar TLDs, such as ".komm" and its similarity to .com, will reportedly be prohibited, Crawford added. Finally, new registries will also be required to implement a "Uniform Rapid Suspension" service where the domain owner can quickly take down a typosquatting offender.

Additional security measures include improved WHOIS listings that will provide a unified database covering every registration in the top-level domain, so that consumers know exactly who owns what. There's also an expectation that certain strings (.bank, for example) would be expected to deploy appropriate levels of security, or else risk harm to consumers.

Still, Crawford noted, consider a company like France's Moet Hennessy Luis Vuitton (LVMH), which could register .lvmh, or .christiandior, or dior.lvmh, or many others. "If you're an organization with thousands of brands, do you need to get a top-level domain for the overall organization, or do a bit of both? There's lots of brand consultancies and branding hierarchy experts working with companies on this," he said. "It's a real challenge."

The complications and expense may seem like gTLDs may be beyond the reach of smaller businesses. In that case, Crawford recommends, businesses should band together.

In the case of .burger, for example, or .law, an industry association could acquire domain names and set policies for them, serving as a registrar as well as an association that would promote the legal profession or fast food, Crawford said.

"Again, it's a question of consumer confidence," Crawford said; people should expect that a business with a ".law" suffix should be a certified professional. "Anyone can buy the domain name '.law'; there's no regulation of any sort. There's some opportunity for a business."

The problem, according to Alan Drewsen, executive director of the International Trademark Association (INTA), is that the gTLD process moved too quickly forward, too fast for trademark holders to respond to the flood of domains. "We would have set a much more measured approach, launched another round, and then taken a step back" to evaluate it, he said.

Representatives of INTA, CADNA and others said they'll try to petition the House subcommittee to reconsider the process. Matsukata also said that CADNA may work to ask Congress to reconsider ICANN's governance, and thus force it to reconsider the gTLD policy.

The really pernicious scenario, according to Mei-Lan Stark, the treasurer of INTA and senior vice president for the Fox Entertainment Group, is that a brand owner turned registry owner may not be able to afford the upkeep of the TLD, and may want to walk away. In such a scenario, ICANN may reassign the gTLD.

"That may have no significance beyond the financial loss if the registry is generic, e.g. .film, but what if the brand owner acquired .brand?" where .brand represents the company's name, Stark said, in prepared remarks. "ICANN could sell that valuable piece of intellectual property to a competitor, to a third party, or to a third party with bad intentions. Any of those results will ruin, not just diminish the value of the brand."

In other words, Stark said, the brand owner would be forced to continue to operate the registry and not be able to get out. "This would be a disaster for the brand and its consumers," she said.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.